FortiDeceptor: Understanding the Rapid Expansion of the Deception Technology Market

Alexander Holzer, CSE

Deception Technology

Why now?

Why Now - Well-defined and Proven Technology

Cyber Deception Technology is recognized by Gartner as the most effective method to detect advanced threats

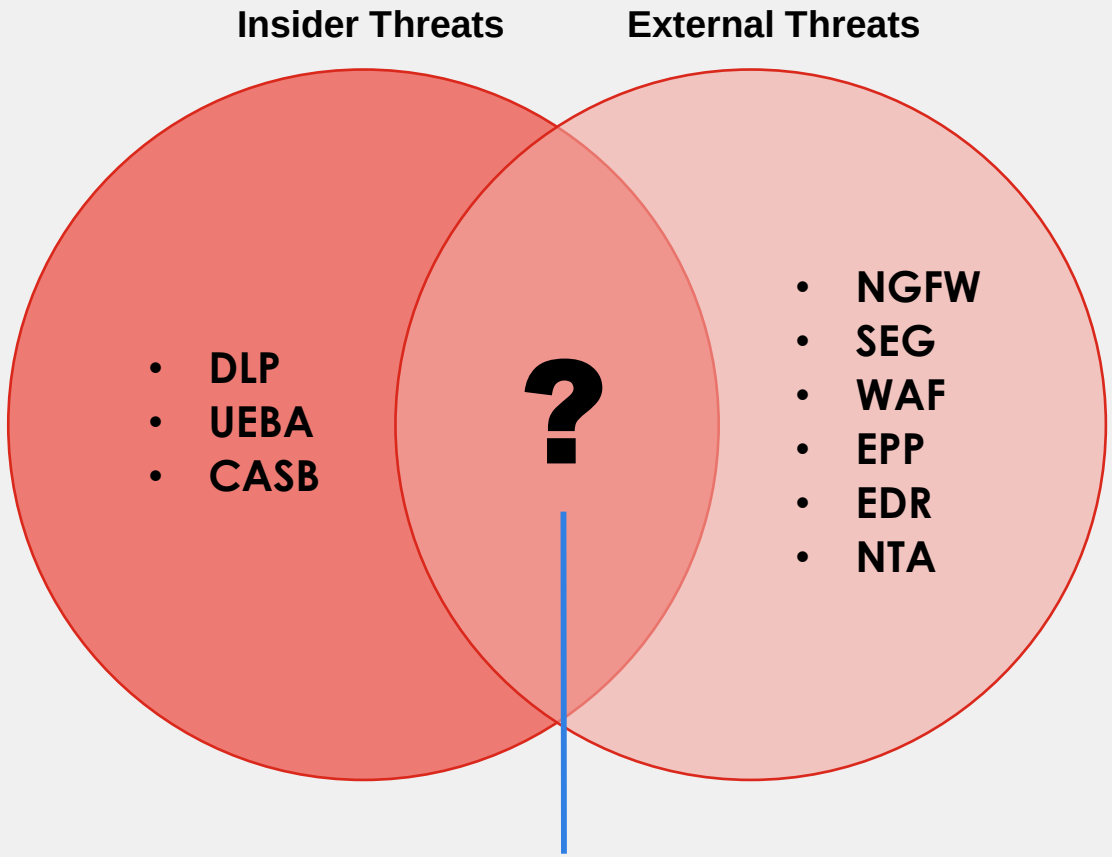
"Prioritize deception-based detection approaches for environments that cannot use other security controls due to technical reasons (for example, IoT, SCADA or medical environments) or due to economic reasons (for example, environments with highly distributed networks)."

* Gartner Hype Cycle for Threat-Facing Technologies, 2018

"Security organization dealing with skill-set shortages are prioritizing low friction approaches such as Deception over resource intensive approaches such as SIEM, UEBA, EDR or NTA".

* Gartner Hype Cycle for Threat-Facing Technologies, 2018

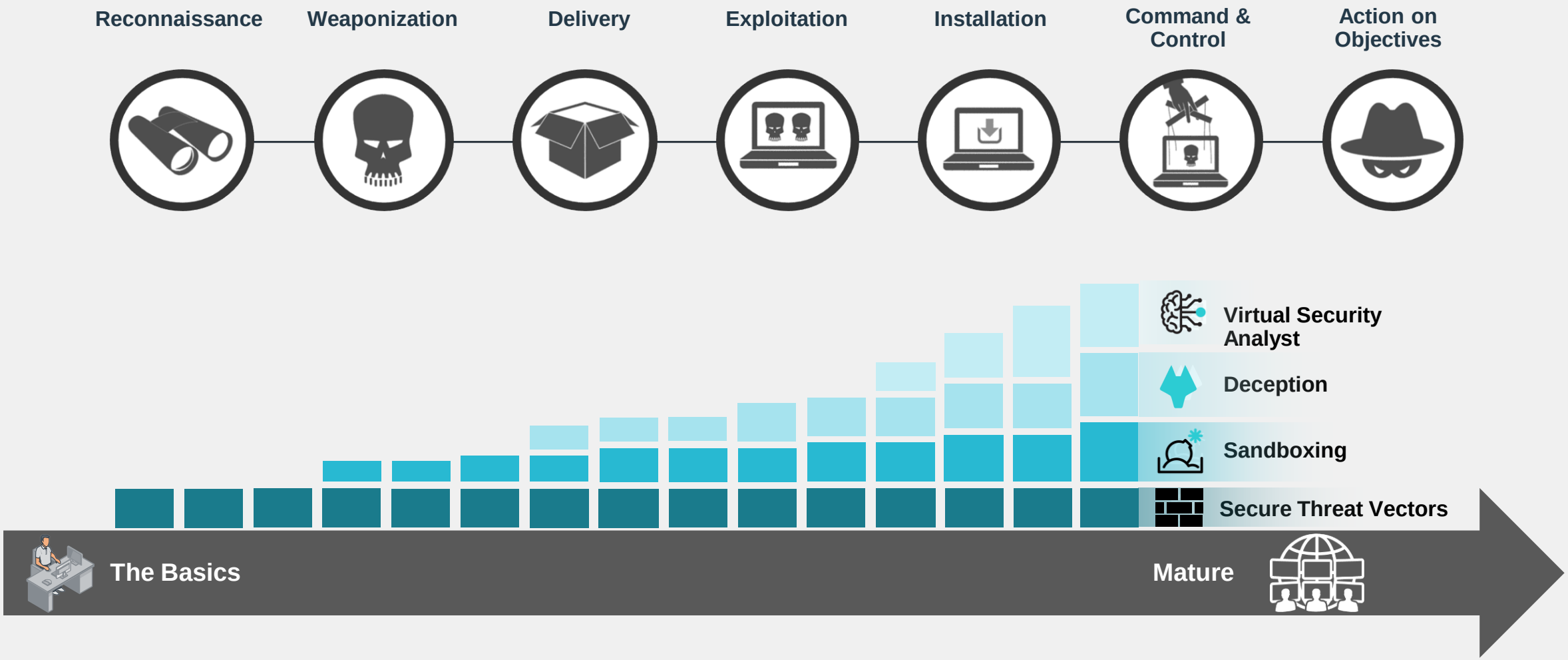
A Two Solution Breach Protection Approach



A solution for BOTH external AND internal threats

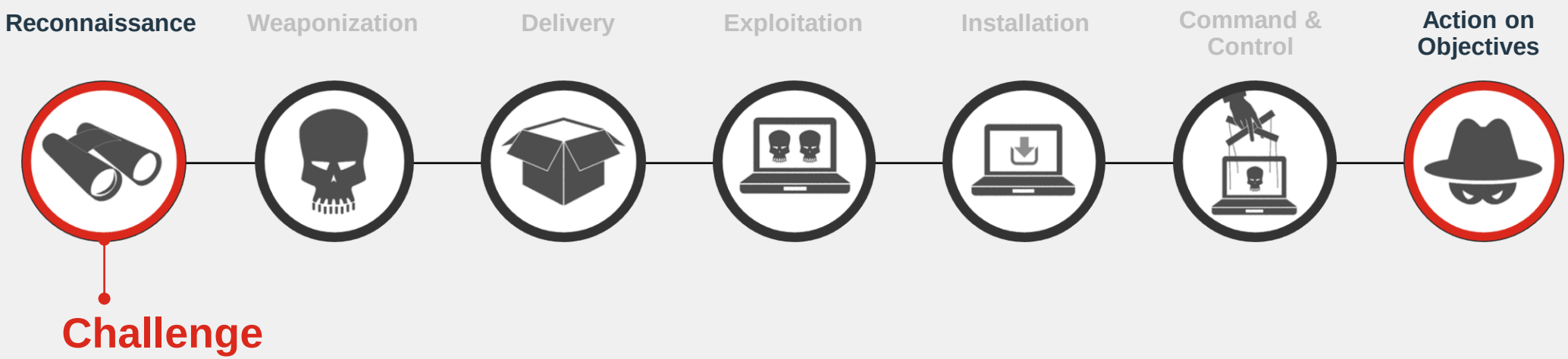
Security Framework for Digital Security

SOC Maturity Model



Deception

Disrupt Threat Actors



External & Internal Actors

Mitigation Cost

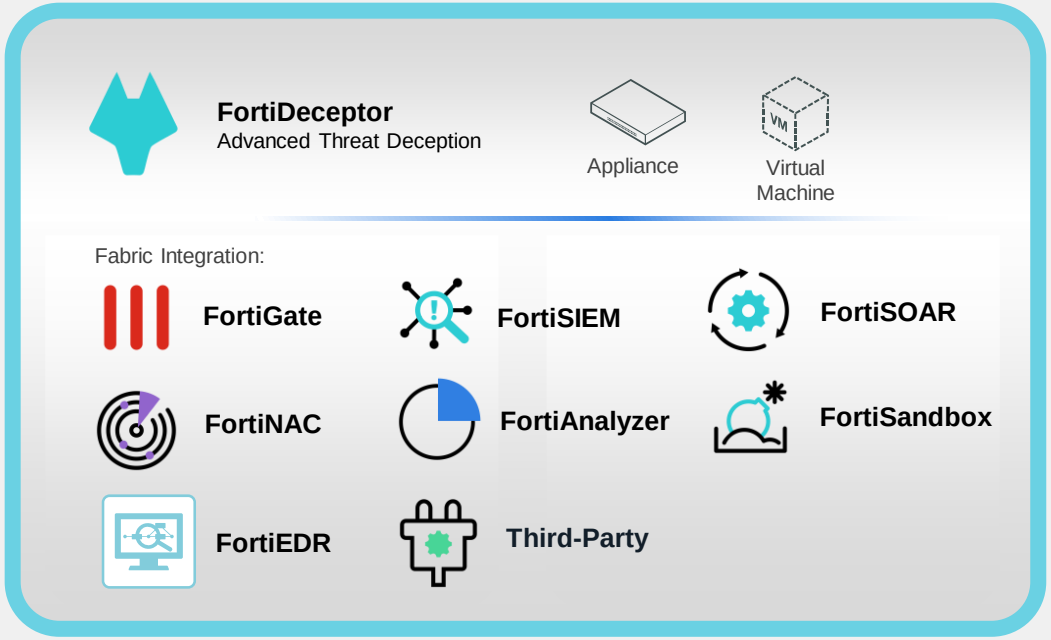
Deception

Disrupt Threat Actors

Solution

Deception

An advanced threat deception designed to DECEIVE, EXPOSE, and ELIMINATE external and internal threats early in the attack kill chain and proactively block these threats before any significant damage occurs.



Honeypot vs Deception

	Traditional Honeypot	Deception (Honeypot 2.0)
Deployment options		
Threat Actors		
Authenticity		
Capture Lateral Movement		
Automated Threat Response		

FortiDeceptor Technology

AI-driven Security Operations

DECEIVE | EXPOSE | ELIMINATE

Decoys & Lures

- Rich offering of Deception Decoys.
- Rich offering of Deception lures to expand the attack surface.
- Deception Decoys & lures deployment automation.

Incident Analysis & Threat intelligence

- Alert analysis automation
- Malware analysis automation
- Generate Threat & actionable intelligence IOC's

Fabric integration

- Fortinet Fabric support for Mitigation & Remediation
- Generic REST-API wizard builder to integrate with any third part tools for Mitigation & Remediation

System Features

- Enterprise management console
- Security reporting and analytics
- Support air-gap networks deployment
- SIEM support

FortiDeceptor: Overview

An advanced threat deception designed to DECEIVE, EXPOSE, and ELIMINATE external and internal threats early in the attack kill chain and proactively block these threats before any significant damage occurs.

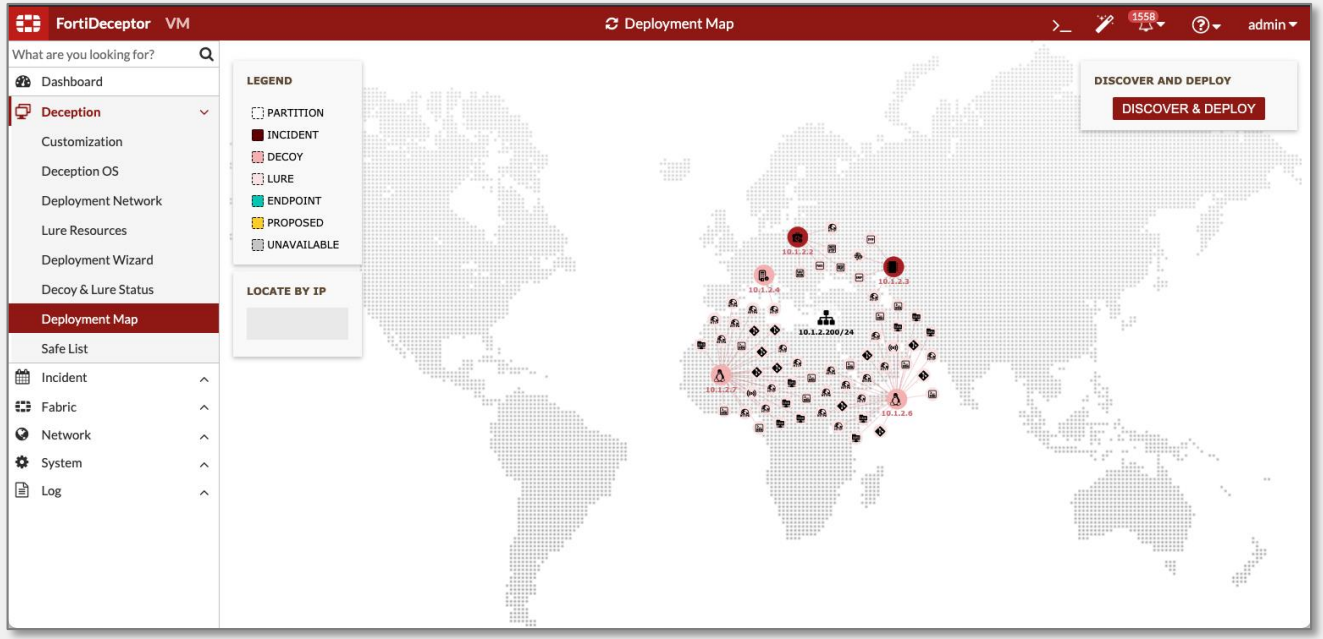
FortiDeceptor
Advanced Threat Deception

Appliance

Virtual Machine

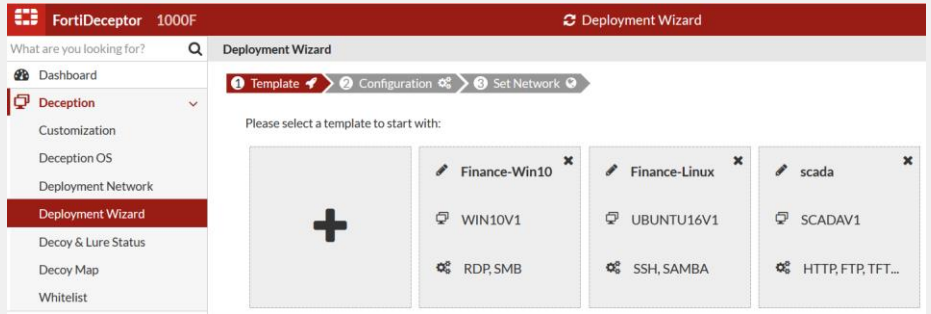
Fabric Integration:

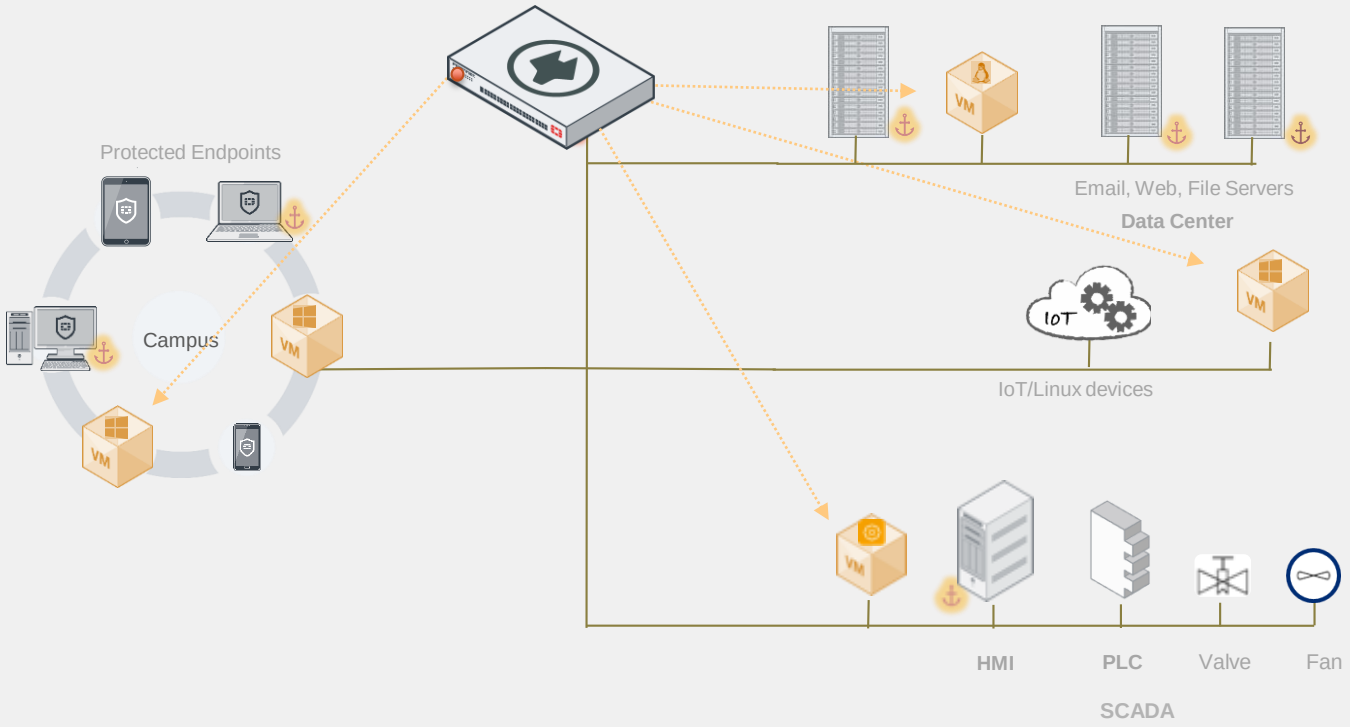
- **FortiGate**
- **FortiSIEM**
- **FortiSOAR**
- **FortiNAC**
- **FortiAnalyzer**



FortiDeceptor: LifeCycle

Deceive



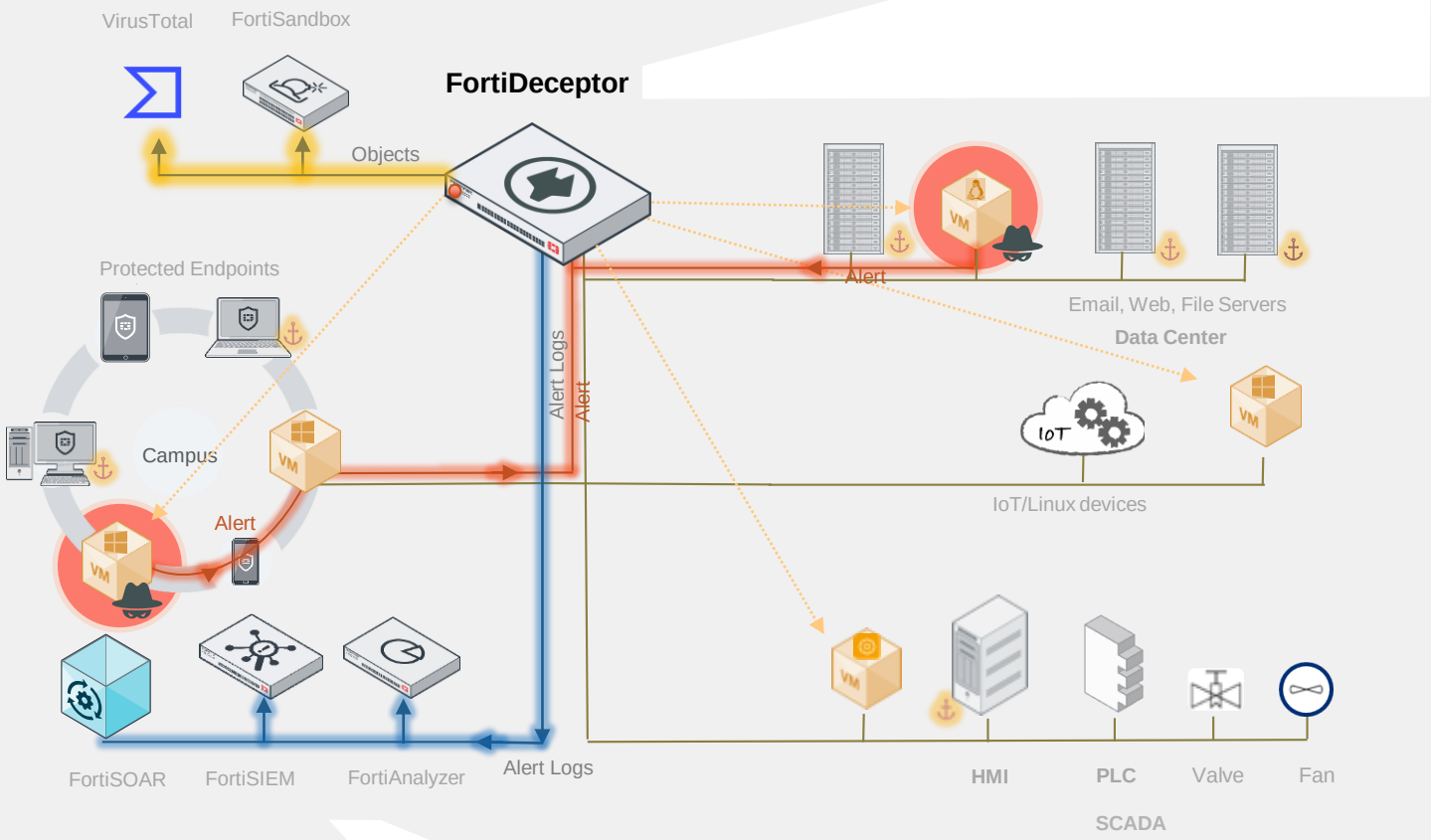


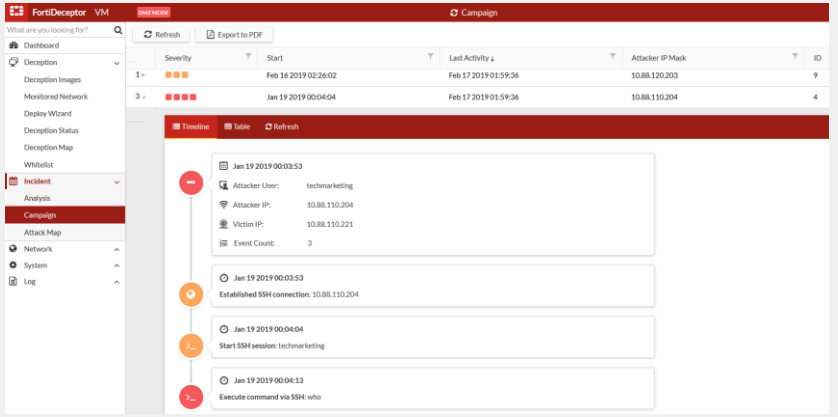
- Lure attackers to decoys that appear indistinguishable from real IT and OT assets and are highly interactive
- Centrally manage and automate the deployment of decoy VMs (Windows, Linux, ICS/SCADA) and generation of lures (data, application /services*)

OT Lures: MODBUS, S7-200, IPMI, Bacnet, Triconex, Guardian-AST, IEC104, ENIP, DNP3
IoT Lures: Medical PACS, DICOM, infusion pump, ERP, POS, GIT, router, camera, printer
IT Lures: SSL VPN, RDP, SMB, SQL, SSH, SAMBA, honeydocs (office, pdf), etc.

FortiDeceptor: LifeCycle

Deceive > Expose

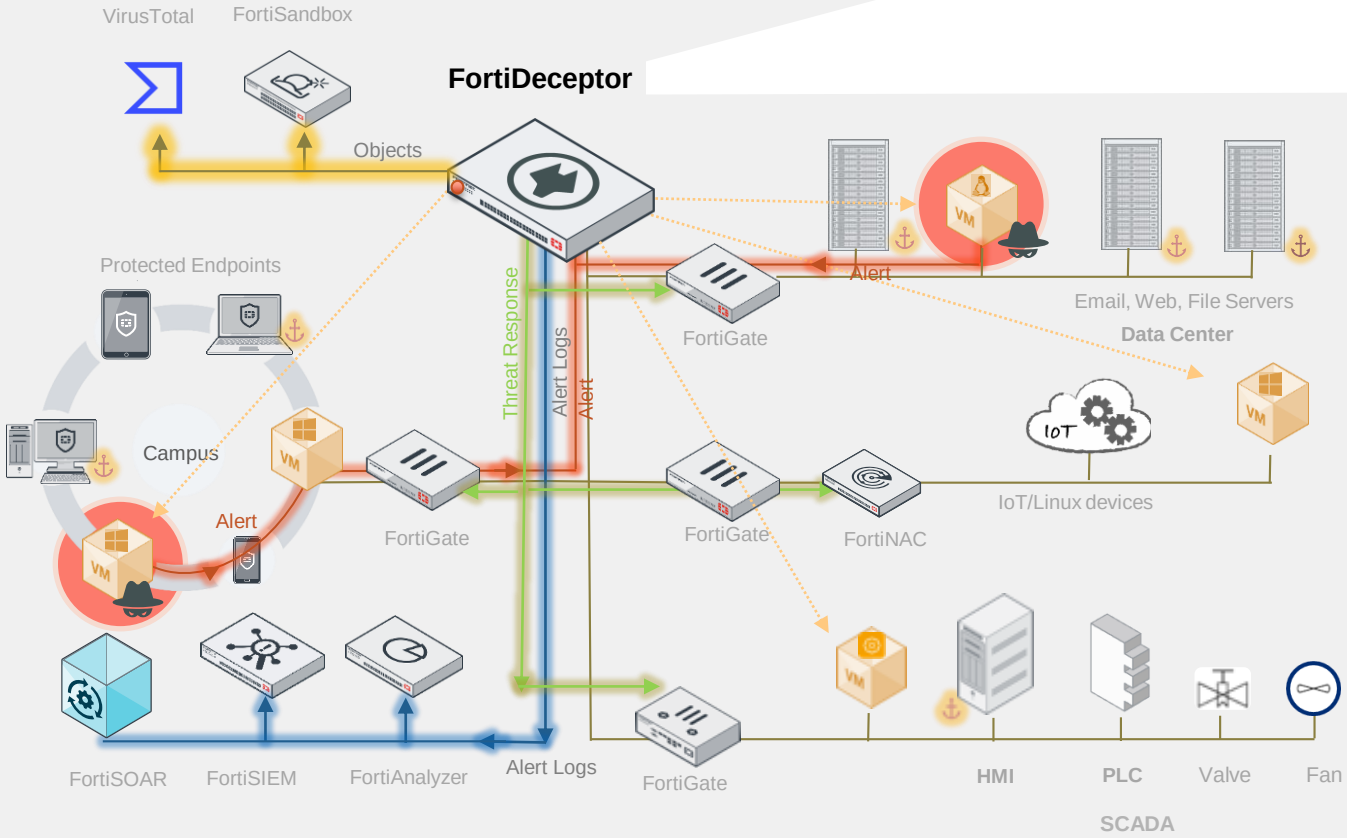


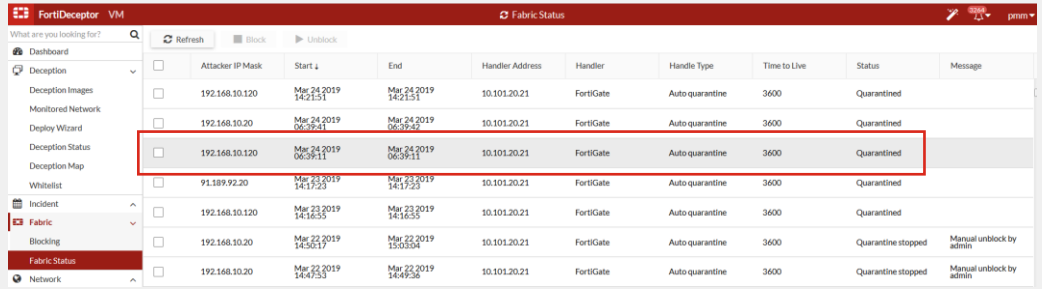


- Acts as an early warning system that generates alerts for review and validation
- Malware tactics validated via VirusTotal, FortiSandbox, Ransomware responder
- Consolidate detection and correlation of external and internal actor activities into a single pane view of threat campaign

FortiDeceptor: LifeCycle

Deceive > Expose > Eliminate





- Manual/Automatic severity-based blocking of attackers before any real damage occurs
- Fabric integration
  - FortiGate: Quarantine IP address
  - FortiNAC: Isolate devices
  - FortiSOAR: Trigger playbooks
  - FortiSIEM: Visibility and threat hunting
  - 3rd Party: Fabric Connector

FortiDeceptor – Use of Tokens

To increase “Deception Surface” or catch rate

Tokens For Example, RDP, SMB, SSH credentials installed on real endpoints

Example: Option 1

80 real PCs/Servers on network, **20** Decoy VMs deployed

Deception Surface/Catch rate = **20%**

20% chance of attacker hitting a Decoy and get caught

Example: Option 2 (**RECOMMENDED**)

80 real PCs/Servers on network, **with token packages installed**, 20 Decoy VMs deployed

Deception Surface/ Catch rate = 100%

100% catch rate - If any attackers hit a real server (and access tokens) **or** Decoy VMs, they will be caught!

Also consider the real endpoint might be compromised and used by attackers

FortiDeceptor Core Technology

Intrusion Detection

- Based on FortiGuard IPS service
- Detect Attacks TO and FROM Decoys

Anti-Malware

- Malware scan on executables dropped
- PCAP downloadable

Web Filtering

- Based on FortiGuard Web Filtering engine
- Rate websites visited on Decoys by Attackers / further downloads

- Anti-Reconnaissance & Anti-Exploit Engine (ARAE)
- Real-Time Tracking of Attackers Activities
- Correlate Campaigns

FortiDeceptor As Part of The Fabric

Deception-enabled Fabric

Broad

Fabricated network of decoys deployed across both IT and OT segment to expose attackers

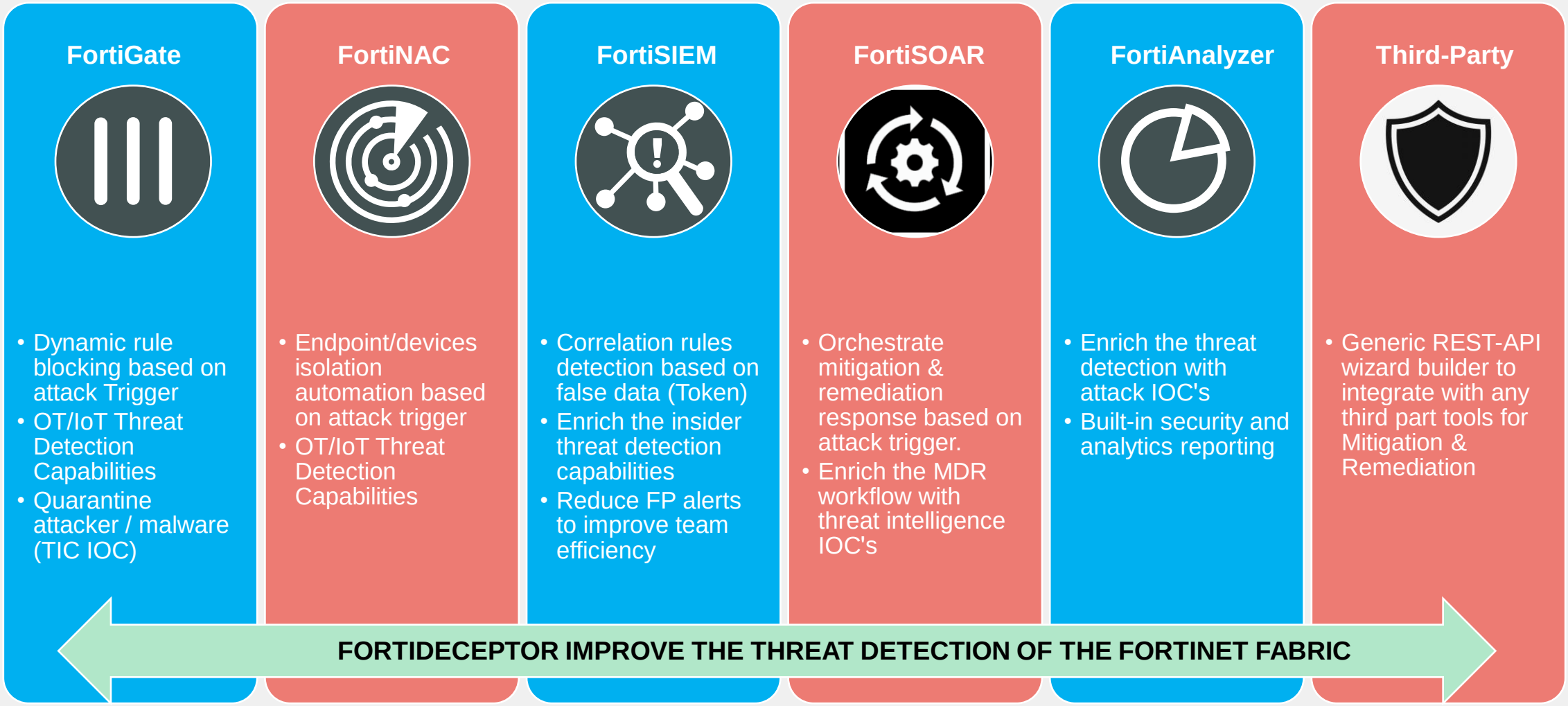
Integrated

Analytics with AI-based detection serves as an early warning of an impeding threat campaign

Automated

Response to attacks through integration of in-line security controls before irreparable damage occurs

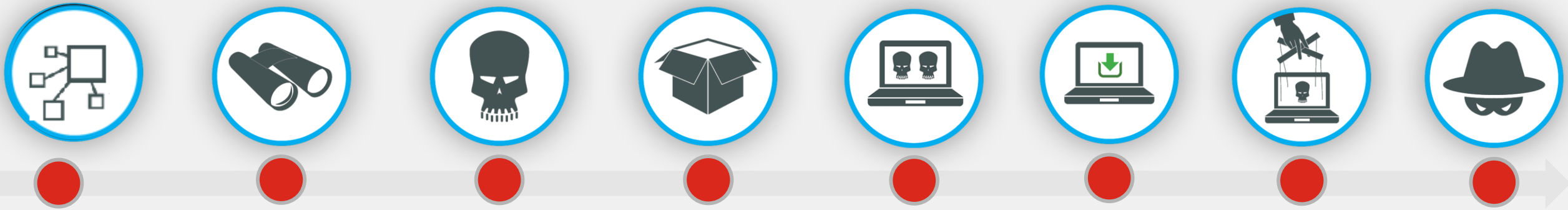
FortiDeceptor As Part of the Security Fabric



FortiDeceptor Use Cases & MITRE Engage

The MITRE Shield Matrix – FortiDeceptor Coverage

https://shield.mitre.org/tactics/



CHANNEL

- Admin Access
- Application Diversity
- Decoy Account
- Decoy Content
- Decoy Credentials
- Decoy Network
- Decoy Persona
- Decoy Process
- Decoy System
- Detonate Malware
- Network Diversity

COLLECT

- Application Diversity
- Decoy Account
- Decoy Content
- Decoy Credentials
- Decoy Network
- Decoy Persona
- Decoy Process
- Decoy System
- Network Diversity
- PCAP Collection

CONTAIN

- Admin Access
- Decoy Account
- Decoy Network
- Detonate Malware
- Isolation

DETECT

- Application Diversity
- Decoy Account
- Decoy Content
- Decoy Credentials
- Decoy Network
- Decoy System
- Detonate Malware
- Isolation
- PCAP Collection

DISRUPT

- Admin Access
- Application Diversity
- Decoy Content
- Decoy Credentials
- Decoy Network
- Detonate Malware
- Isolation

FACILITATE

- Admin Access
- Application Diversity
- Decoy Account
- Decoy Content
- Decoy Credentials
- Decoy Diversity
- Decoy Network
- Decoy Persona
- Decoy System
- Network Diversity

LEGITIMIZE

- Application Diversity
- Decoy Account
- Decoy Content
- Decoy Credentials
- Decoy Diversity
- Decoy Network
- Decoy Persona
- Decoy Process
- Decoy System
- Network Diversity

TEST

- Admin Access
- Application Diversity
- Decoy Account
- Decoy Content
- Decoy Credentials
- Decoy Diversity
- Decoy Network
- Decoy Persona
- Decoy System
- Detonate Malware
- Network Diversity

FDC COVERAGE FOR MITRE SHIELD MATRIX

Deception Use Cases – Enrich The Fortinet Product Offering

Lateral Movement Use case

- Detecting threats moving inside the network, as opposed to detecting threats on egress/ingress
- Employing detection as a last-resort security control (that is, "detect when all other controls fail")
- Enabling a defense-in-depth & active defense strategies

OT/ IoT Use case

- Network Visibility & Breach detection through passive footprint
- Detecting threats to assets that cannot provide their own telemetry such as IoT, SCADA and MEDICAL devices

Threat Hunting

- Enabling less noisy threat detection inside the network to empower your SOC team
- Leveraging Deception Lure to track the origin of an attack
- Learning about attacker TTPs by observing attackers in highly monitored environments, where there is no pressure to kick them out

FortiDeceptor Decoys and Lures

Deception OS & Deception Decoys

Windows Decoys:
- Win 7
- Win 10 Pro

Linux Decoys:
- Ubuntu
- CentOS

Custom Decoys:
- Win 10 Pro
- Win Server 2016
- Win Server 2019

Cloud:
- AWS
- AZURE
- GCP

FortiGate (SSLVPN):
- FGT-60E
- FGT-100F
- FGT-1500D
- FGT-2000E
- FGT-3700D

Application OS:
- CRM/ERP
- POS
- GIT (Linux)
- SQL and HTTP (Win)
- SAP

Medical OS:
- PACS
- DICOM
- Infusion Pump

IoT OS:
- HP/Lexmark/Brother
- IP Cam
- Cisco Router

SCADA OS:
- UPS
- S7
- BACnet
- ....

SCADA Deception Decoys & Deception Lures

SCADA Decoys:

- Siemens S7-200
- Siemens S7-300
- Schneider PM5560
- Schneider EcoStruxure BMS server
- Schneider ScadaPack 333E
- Rockwell
- IPMI Device
- Kamstrup 382
- VAV-DD Bacnet controller
- Guardian AST
- Ascent Compass MNG
- ....

SCADA Lures:

- HTTP
- FTP
- TFTP
- SNMP
- Modbus
- S7Comm
- ENIP
- Bacnet
- IPMI
- Triconex
- Guardian-AST
- IEC104

Available Deception Lures & Token

Windows Endpoint:

- SMB
- RDP
- ICMP
- NetBIOS
- Cached Credentials
- Fake Network Connect

Linux Endpoint:

- SMB
- SSH
- HTTP/HTTPS
- GIT
- TCP Listener
- ICMP
- Cached Credentials

MAC Endpoint:

- SMB
- RDP
- SSH

Custom Decoys & Lures

Supported custom OS

- Windows 10
- Windows Server 2016/2019
- Windows Server 2016/2019 with customized MSSQL and IIS service

- **Supported custom Lure-Resource**
- LDAP username import & creating fake passwords (TCP 389)
- Import usernames & passwords (from txt-file)
- Import custom honey docs

Licensing

FortiDeceptor VM – Subscription License

Subscription-based License-bundle concept to cover all the FortiDeceptor modules under 1 SKU that will be priced based on the number of network Deception VLANs.

Base license:

- SKU = FC1-10-DCVMS-496-02-DD
- Virtual appliance (max. 20 Deception VMs)
- FortiCare 24 X 7
- FortiGuard Services Subscriptions (ARAE)
- Custom decoy
- All network decoys & All Windows decoys (Windows license excluded).
- All Deception Lures
- Pricing per VLAN, minimum order of 2 VLANs (max. 128 VLANs)
- Custom decoys (Deploy of Windows decoy with BYOL license)

FortiDeceptor VM – Subscription License

Additional licenses:

FortiDeceptor Windows License (perpetual):

- SKU = LIC-FDC-WIN
- 1 X win7 and 1 X win10 decoys
- License is flexible and allows to deploy both license for the same OS

FortiDeceptor Central Management license:

- SKU = FC-10-FDCCM-497-02-DD
- License for FDC manager in case customer needs to manage remote appliances
- Management of up to 50 FortiDeceptor devices

Summary

BREACHES
External and Internal threats

EARLY WARNING
High Fidelity Alerts, Redirect Attackers, Threat Analysis and Response

FABRIC INTEGRATION
Block Threats Automatically & Actionable Intelligence

BROAD COVERAGE
IT and IoT/OT Networks

EASE OF USE
Wizard-based provisioning and deployment, simple management


FORTINET